OIPE JC 131
JUL 11 2005
PATENT & TRADEMARK OFFICE

AP ZRW

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	09/419,828
Filing Date	October 14, 1999
First Named Inventor	Van Dyke
Art Unit	2137
Examiner Name	M. Smithers
Attorney Docket Number	00100.01.7084

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Vedder, Price, Kaufman & Kammholz, P.C.		
Signature	Patrick B. Law		
Printed name	Patrick B. Law		
Date	July 8, 2005	Reg. No.	41,549

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Patrick B. Law		
Typed or printed name	Patrick B. Law	Date	July 8, 2005

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE JC131 JUL 11 2005 PATENT & TRADEMARK OFFICE

PTO/SB/17 (10-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2005

Effective 10/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500

Complete if Known	
Application Number	09/419,828
Filing Date	October 14, 1999
First Named Inventor	Van Dyke
Examiner Name	M. Smithers
Art Unit	2137
Attorney Docket No.	00100.01.7084

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 50-0441

Deposit Account Name: ATI International SRL

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	790	2001	395	Utility filing fee	
1002	350	2002	175	Design filing fee	
1003	550	2003	275	Plant filing fee	
1004	790	2004	395	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below		Fee Paid
Total Claims		-20** =		X	=
Independent Claims		- 3** =		X	=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	88	2201	44	Independent claims in excess of 3
1203	300	2203	150	Multiple dependent claim, if not paid
1204	88	2204	44	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	430	2252	215	Extension for reply within second month	
1253	980	2253	490	Extension for reply within third month	
1254	1,530	2254	765	Extension for reply within fourth month	
1255	2,080	2255	1,040	Extension for reply within fifth month	
1401	340	2401	170	Notice of Appeal	
1402	340	2402	170	Filing a brief in support of an appeal	500.00
1403	300	2403	150	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,370	2453	685	Petition to revive - unintentional	
1501	1,370	2501	685	Utility issue fee (or reissue)	
1502	490	2502	245	Design issue fee	
1503	660	2503	330	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 500

SUBMITTED BY

(Complete *(if applicable)*)

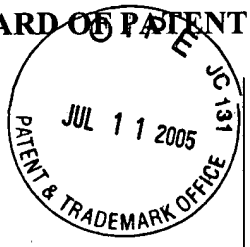
Name (Print/Type)	Patrick B. Law	Registration No. (Attorney/Agent)	41,549	Telephone	312-609-7799
Signature				Date	July 8, 2005

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES



In re application of: Van Dyke et al.	Examiner: M. Smithers
Application No.: 09/419,828	Group Art Unit: 2137
Filed: October 14, 1999	Our File No.: 00100.01.7084
For: ENCRYPTION/DECRYPTION INSTRUCTION SET ENHANCEMENT	Docket No.: M–7084 US

APPEAL BRIEF PURSUANT TO 37 C.F.R. § 41.37

Dear Sir:

Appellants submit this brief further to the Notice of Appeal filed May 8, 2005, in the above-identified application.

I. Real Party in Interest

ATI International, SRL is the real party in interest in this appeal by virtue of an executed Assignment from the named Inventors of their entire interest to ATI Technologies, SRL. The Assignment evincing such ownership interest was recorded on October 14, 1999, in the United States Patent and Trademark Office at Reel 010325, Frame 0492.

II. Related Appeals and Interferences

To Appellant's knowledge, there are no related Appeals or Interferences filed, pending, or decided.

III. Status of Claims

The originally filed Application contained claims 1-21. During prosecution, claims 2 and 14 were cancelled and claims 22-23 were added. Additionally, claims 1, 13, and 15 were amended during prosecution of the present application. All of the pending claims 1, 3-13, and 15-23 are currently rejected under 35 U.S.C. § 102(e). A copy of appealed claims 1, 3-13, and 15-23 is attached in Appendix A below. Of the pending claims, 1, 13, and 22 are independent.

07/12/2005 MBERHE 00000036 500441 09419828
01 FC:1402 500.00 DA

Applicants note typographical errors in appealed claim 23 and have filed an amendment prior to this brief under 37 C.F.R. §1.116 to cure the typographical errors such that claim 23 depends on claim 22 and not claim 1, and is an apparatus claim, not a method claim, in order to put the claim in better condition for this appeal.

IV. Status of Amendments

A "Request for Reconsideration" was filed on April 8, 2005 in response to the final Office Action mailed on February 8, 2005. No amendments were made to the claims, however, subsequent to the final Office Action. The claims listed in Appendix A reflect the claims as they stood at the time the final Office Action was mailed.

V. Summary of Claimed Subject Matter

The claimed subject matter is generally directed to apparatus and methods for performing encryption or decryption under a data encryption standard (DES) algorithm using a type of general processing system. (Page 1, lines 9-11). (See e.g., Figs. 3 and 4 in Appendix B and pages 5-9 of the present specification and, in particular, page 5, lines 20-27). In the described embodiment, general purpose registers of a general purpose processor are used to carry out encryption and decryption, as opposed to, for example special purpose registers used by dedicated encryption/decryption chips. (Page 5, lines 27-34). With this approach also, the disclosed apparatus and methods achieve a speed improvement by an order of magnitude over software implementations of the DES algorithm. (Page 5, lines 34-37).

In particular, an exemplary computer system disclosed in the present application includes a general purpose type processor that is adapted with additional hardware 309 for executing a DSTEP instruction of the DES algorithm and uses general purpose registers of the processor. (Page 6, lines 3-6 and FIGs. 3 and 4). The general purpose processor includes three arithmetic logic units ("ALUs") 302, 304, and 306 (FIGs. 3 and 4 and Page 6, lines 28-33) of which hardware 309 is a part (FIGs. 3 and 4 and Page 7, lines1-6. The ALUs include logic for executing expansion permutation, S-box substitution, P-box permutation, and associated XOR operations. (See FIGs. 3 and Page 7, line 6 – Page 8, line17). A general purpose register file

330 stores and provides operands to the ALUs 302, 304 and 306. (See FIG. 3 and page 5, lines 20-23). The general register file 330 also stores states of the DES algorithm including control, L_i's, R_i's, and subkeys K_i's. (See page 5, lines 24-25).

VI. Brief Summary of the Prior Art Reference

As it is understood, U.S. Patent No. 6,088,800 to Jones et al. (hereinafter "Jones") is directed to a dedicated encryption processor with shared memory interconnect. (See abstract.) The dedicated encryption device, integrated into a single chip, is a dedicated, single purpose processor system whose instruction set is optimized for common encryption algorithms (Jones, col. 3, lines 32-35), and is not a general purpose type processor. In particular, Jones distinguishes that his disclosed encryption processor is different from general purpose processing by stating that "[general purpose processing systems] are not required for encryption, an embodiment of the present invention uses a simpler linear arrangement of the [processing elements] with much less switching circuitry." (Jones, col. 10, lines 20-29). An example of the linear arrangement pipeline is shown in FIG. 2 of Jones, the pipeline being made up of a plurality of processing elements 37 arranged in a linear array, each containing an instruction memory, a register file, and ALU, local and shared data memory, and control circuitry. (Jones col. 6, lines 10-13) Processing elements 37 each consist of an ALU 56 operating on 32 bit words from a register file 58 made up of 8 to16 32-bit registers. (Jones col. 7, lines 17-19). The register file 58 and ALU 56 are controlled by a control unit 60 that decodes instructions from a processing element instruction memory 62. (Jones col. 7, lines 19-22). Each processing element instruction memory stores at least one round of an encryption algorithm, where a round is defined as a sequence of instructions in an encryption algorithm. (Jones col. 7, lines 22-25).

The basic concept behind Data Encryption Standard (DES) as disclosed in Jones, as illustrated in FIG. 14, consists of a substitution followed by a permutation on the text based on the key. (Jones, col. 17, lines 3-5.) The 64-bit block is divided into two 32-bit pieces 108, 110. (Jones, col. 17, lines 7-8.) One piece is unaffected by the encryption. (Jones, col. 17, lines 8-9.) The piece that is affected is divided into eight groups of four bits. (Jones, col. 17, lines 10-11.) Each group is expanded by coping the two bits adjacent to it. (Jones, col. 17, lines 11-12.) Each expanded group is XOR'ed at 112 with a subkey. (Jones, col. 17, line 14.) The six-bit result of the XOR is used to indicate a 64-entry X 4-bit. (Jones, col. 17, lines 15-17.)

VII. Grounds of Rejection to be Reviewed on Appeal

The issue on appeal is whether claims 1, 3-13, and 15-23 are anticipated under 35 U.S.C. § 102(e) by Jones.

VIII. Argument

The rejections of claims 1, 3-13, and 15-23 should be reversed because the Final Office Action mailed February 8, 2005 ("final Office Action") failed to establish that Jones teaches each and every element as set forth in the claims. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Further, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

A. THE ANTICIPATION REJECTION MUST BE REVERSED SINCE JONES FAILS TO TEACH ALL OF THE ELEMENTS SET FORTH IN THE CLAIMS

1. Claim 1

Appellants submit that Jones does not teach or suggest each and every element of independent claim 1 including, *inter alia*, "...an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations; wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and wherein said register file includes general purpose registers." In particular, Appellants submit that Jones does not teach or suggest, *inter alia*, using "general purpose registers," but rather specific purpose registers in a dedicated encryption/decryption processor to avoid using general purpose type processors. (See Jones, col. 10, lines 20-29).

As discussed above, Jones is directed to an encryption device integrated into a single chip, which is a dedicated, single purpose processor system whose instruction set is optimized for common encryption algorithms and suggests away from general purpose processing for

encryption algorithms, such as DES. (See Jones, col. 10, lines 20-29).). Additionally, Jones discusses that the disclosed, dedicated encryption processor is faster than a software implementation on a conventional CPU (e.g., a general purpose processing system), thus evincing that Jones suggests away from general purpose processors. (See Jones, col. 18, lines 14-16). In contrast, the present application utilizes a type of general purpose microprocessor and associated general purpose registers for carrying out a DES algorithm with general purpose instructions of the general purpose microprocessor, which inherently may be used to execute instructions other than the DES algorithm. (See pg. 5, lines 20-27 of the present specification). States of the DES algorithm are stored in general purpose registers, thereby eliminating special purpose modules (i.e., registers) of the known prior art, as well as achieving high performance by executing part of the DES instruction in the general purpose hardware. Thus, it would not make sense with the dedicated processor system of Jones to utilize "general purpose registers" as featured in claim 1.

The particular sections of Jones referenced by the Examiner in the rejection of claim 1 (i.e., col. 6, lines 3-13; col. 7, lines 15-38; col. 16, line 57 through col. 18, line 13; and figures 2, 4, 5, 6 and 14) are alleged to disclose "wherein said register file includes general registers." Appellants submit, however, that these sections of Jones do not actually teach the use of a general purpose register for providing operands to an arithmetic logic unit that operates as claimed. Rather, Jones merely teaches that the register file 58, for example, is made up of 8-16 32-bit registers as part of a dedicated encryption/decryption register set. Jones does not teach use of any general purpose registers as he does not use a general purpose type processor. Moreover, Appellants note that after a word search of the Jones patent, the explicit claim terminology of "general purpose registers" is not found anywhere in the patent. Thus, the assertion that the claimed "general purpose registers" are explicitly disclosed by Jones is either inaccurate or a mischaracterization of the teachings.

Furthermore, Appellants submit that the teaching in Jones of an array of processing elements at column 3, lines 45 through 66, is precisely the prior art described in the Background of the invention in the present application. For example, the present specification states:

> as the encryption/decryption process of the DES algorithm of FIG. 1 is too computationally demanding for a software implementation on a general

> purpose microprocessor, the DES algorithm is often implemented by *an array of identical special purpose modules* outside of the microprocessor. However, several drawbacks are inheriting such an approach. First, partitioning the encryption/decryption tasks between the microprocessor and the special purpose modules is complex, especially since the different instruction sets are executed by the microprocessor and the special purpose modules.

(Specification, page 3, lines 25-35 (emphasis added).) The DES algorithm of claim 1 is implemented with general purpose registers, not with the special purpose modules of the prior art. (Specification, page 4, lines 31-33.) For example, the DES algorithm may be implemented on a type of general purpose microprocessor while storing the states of the DES algorithm in general purpose registers, rather than, special purpose modules of the prior art. (Specification, page 5, lines 20-30.) A general purpose register is usually explicitly addressable, with any set of registers, and can be used for different purposes, for example, as an accumulator, as an index register, or as a special handler of video or used for other non-encryption/decryption purposes. As such, Appellants submit that Jones's disclosed use of ALU 56 operating on 32-bit words from the register file 58 does not disclose, teach or suggest Appellants claimed subject matter including at least "wherein said register file includes general purpose registers."

Appellants wish to also note that in the final Office Action, the Examiner asserted that the Appellants had previously argued in the Amendment of August 31, 2004, that Jones does not disclose a register file providing operands to an ALU. This was not Appellants' argument. More correctly, Appellants' argument was that Jones does not disclose a general purpose register for providing operands to an ALU. Additionally, the Examiner alleged in the final Office Action that col. 7, line 65 through col. 8, line 29 of Jones "makes it clear that any register can be used to enhance the instruction set performing the necessary operations within the cryptographic procedure" (emphasis added). By referencing this particular part of Jones, it appears that the Examiner is alleging that this teaching is commensurate with a teaching of general purpose registers. Appellants respectfully submit, however, that the import of the cited section of Jones, read properly in light of its context, is not teaching the use of any ***type*** of register, which could include a general purpose register, but rather that any of the special purpose registers 58 in the processing elements 37 taught by Jones can be used as an operand to any instruction given that

the instruction set of Jones is more or less orthogonal. That is, the PE instruction memory 62 may provide an instruction set to any of the register files 58 through the control unit 60 in any of the processing elements 37. One of ordinary skill in the art, reading the cited section in its context, would not equate the language "any register" as being any type of register, but instead any of the special purpose registers 58 within the processing elements 37 being able to receive the instruction set from the PE instruction memory 62. Accordingly, the Appellants respectfully submit that this reasoning presented in the final Office Action is not tenable and that Jones, in fact, does not teach or suggest the use of general purpose registers.

b. Claim 3

Appellants submit that Jones does not teach or suggest Appellants' claim 3 subject matter including, *inter alia*:

> "... said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey"

(claim 3). The Office Action makes reference to Jones at col. 6, lines 3-13; col. 7, lines 15-38; col. 16 lines 57 to col. 18, line 13 and figures 2, 4, 5, 6 and 14 as disclosing Applicant's claim 3 subject matter. The Examiner's repeated block citation to Jones in reference to rejecting each and every element of all the claims fails to show the particular part in Jones relied on and fails therefore to provide the alleged limitation by limitation analysis of the claims and also fails to show the part of Jones relied on for the rejections as required by 37 C.F.R. § 1.104(c)(2)[1]. Appellants submit that what Jones discloses in Jones at col. 6, lines 3-13; col. 7, lines 15-38; col. 16 lines 57 to col. 18, line 13 and figures 2, 4, 5, 6 and 14 is a description of *inter alia* of ALU 56 operating in 32-bit words from the register file 58 with 16 by 32-bit registers. (Jones col. 7, lines 17-19). As a result, Jones as cited is absent any discussion of using a first, second and third register in the manner claimed in Appellants' claim 3 subject matter. Therefore, the Appellants

[1] When the reference is complex or shows or describes inventions other than that claimed by the applicant, a particular part relied on must be designated as nearly as practicable 37 C.F.R. § 1.104(c)(2).

hereby request a showing of where Jones teaches each and every element as arranged in the claims. Further, the final Office Action fails to show where Jones teaches 'a third register for storing a subkey." In addition, and as discussed above in regards to claim 1, Jones's discussion in col. 7, lines 17-20 is directed to merely *inter alia* ALU 56 receiving 32-bit words from a register file and as such there is no discussion therein using a first, second and third register in the manner claimed in Appellants' claimed subject matter. Therefore, Appellants submit that Jones does not disclose, teach or suggest Appellants' claimed subject matter.

c. Claim 4

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 4 subject matter including, *inter alia*, "... said datum is 64 bits long and said subkey is 48 bits long" (claim 4). In contrast, Jones teaches that the ALU 56 receives 32-bit words from register file 58 and therefore teaches away from the claimed subject matter "... said datum is 64 bits long and said subkey is 48 bits long." The final Office Action fails to show where Jones teaches among other things "... said datum is 64 bits long and said subkey is 48 bits long." Moreover, Appellant points out that a word search of Jones reveals that no explicit disclosure a subkey being 48 bits long is found anywhere in the patent. Accordingly, Jones fails to teach the elements of this claim.

d. Claim 5

Appellants submit that Jones does not teach or suggest Appellants' claim 5 subject matter including, *inter alia*, "... said first and second portions each contain one-half number of bits of said datum" (claim 5). The final Office Action failed to show where Jones teaches each and every element as arranged in this claim. Rather, the final Office Action merely cited generally to large sections of Jones as teaching these elements. Indeed, Jones does not teach the "first and second portions" as argued previously with respect to claim 3. Thus, Jones cannot meet the elements of this claim. Further, Jones fails to explicitly teach dividing datum in half between registers. Accordingly, Jones fails to teach each and every element of this claim.

e. Claim 6

Appellants submit that Jones does not disclose, teach or suggest Appellants claim 6 subject matter including "wherein each of said first and second portions is 32-bits long." Again, the Office Action cites generally to the same portions of Jones without showing where each and every element as arranged in the claims is taught in Jones. Appellants repeat the relevant remarks made above.

f. Claim 7

Concerning claim 7, Appellants submit Jones does not teach or suggests Appellants' claim 7 subject matter including, *inter alia*:

> "... said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent executing of said instruction." (claim 7).

Here, the final Office Action again makes reference to the stated language in Jones without showing where Jones teaches each and every element as arranged in the claims. Appellants again repeat the above relevant remarks, in particular those remarks directed to the second and third registers. Further, the final Office Action fails to show where Jones teaches "... said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent executing of said instruction."

g. Claim 8

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 8 subject matter including, *inter alia*, "... a bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers" (claim 8). Again, the Office Action makes reference to the stated language in Jones previously cited as disclosing Applicant's claimed subject matter without showing where Jones teaches each and every element in the claims. As discussed above,

not only is such language in Jones absent from any discussion of the use of a register file containing general purpose registers, or first, second and third general purpose registers, Appellants further submit that Jones is also absent discussion on the use of Appellants' claimed bypass mechanism 302–Fig. 3. Therefore, Appellants submit that Jones cannot and does not disclose, teach or suggest Applicant's claimed subject matter.

Additionally, during prosecution Appellants argued that Jones does not teach the claimed bypass mechanism. However, the final Office Action and previous Office Actions failed to address the Appellants' arguments. As a result, the Examiner has continually failed to show where Jones teaches each and every element as arranged in the claims.

h. Claim 9

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 9 subject matter including, *inter alia*, "... said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit" (claim 9). Regarding the same cited language in Jones at col. 6, lines 3-13; col. 7, lines 15-38; col. 16 lines 57 to col. 18, line 13 and figures 2, 4, 5, 6 and 14, Appellants submit that Jones discusses a DES operation generally at col. 16, lines 57 through col. 18 lines 13, but is otherwise absent any discussion of a "bypass mechanism," and therefore does not disclose Appellants' claimed subject matter. Appellants also repeat the relevant remarks made above with regard to claim 8.

i. Claim 10

Appellants submit that Jones does not teach or suggest Appellants' claim 10 subject matter including, *inter alia*,

> "... a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operation in parallel with said logic circuit."

(claim 10). Here, the Office Action again makes reference to the same cited portions of Jones made with all the other claims in the Office Action as disclosed in Appellants claim 10 subject matter. Appellants submit that Jones at col. 16, line 57 through col. 18, line 14 discloses a DES system generally, however the Office Action fails to show where Jones teaches "... a

second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operation in parallel with said logic circuit." Further, the cited portion of Jones teaches DES creates subkeys from a single key, in this case 56-bits. However, the Appellants are unable to find where Jones although discussing the creation of subkeys fails to disclose performing of a key selection parallel with the logic circuit. Therefore, Applicant submits that Jones cannot and does not disclose, teach or suggest Appellants claimed subject matter.

j. Claims 11 and 12 stand and fall together

Concerning claim 11, Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 11 subject matter including, *inter alia*, "... said logic circuit further comprises a circuit for selecting a subkey from a key" (claim 11). Appellants submit also that at least because claim 11 depends from claim 1, and as a dependent claim therefrom, claim 11 is allowable for the reasons claim 1 is allowable. Appellants further submit that claim 11 is also allowable in light of the presence of novel and non-obvious elements contained in claim 11 that are not otherwise present in claim 1.

Appellants submit that at least because claim 12 depends from claim 11, and as a dependent claim therefrom, claim 12 is allowable for the reasons claim 11 is allowable. Appellants further submit that claim 12 is also allowable in light of the presence of novel and non-obvious elements contained in claim 12 that are not otherwise present in claim 11.

k. Claims 13 and 15 stand and fall together

Appellants submit that Jones does not disclose, teach or suggest each and every element of independent claim 13 including, *inter alia*, "wherein said register file includes general purpose registers." (claim 13). For the sake of brevity, Appellants submit that for the same reasons discussed above regarding the reasons why Jones does not disclose, teach or suggest Appellants' claim 1 subject matter, that Jones also does not disclose, teach or suggest all of the elements of claim 13. Namely, Appellants submit that Jones does not disclose, teach or suggest the use of "wherein said register file includes general purpose registers." Therefore, Appellants submit that Jones cannot and does not disclose, teach or suggest Applicant's claimed subject matter.

Appellants submit that at least because claim 15 depends from claim 13, and as a dependent claim therefrom, claim 15 is allowable for the reasons claim 13 is allowable.

l. Claim 16

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 16 subject matter including, *inter alia*,

> "... storing a first portion of a datum for said encryption or decryption in first register in said register file; storing a second portion of said datum for said encryption or decryption in second register in said register file; and storing a subkey for said encryption or decryption in third register in said register file."

(claim 16). Appellants submit that for the same or similar reasons discussed above regarding the reasons why Jones does not disclose, teach or suggest Appellants' claim 3 subject matter, that Jones also does not disclose, teach or suggest Appellants' claim 16 subject matter. Therefore, Appellants submit that Jones cannot and does not disclose, teach or suggest Appellants' claimed subject matter.

Appellants submit that at least because claim 16 depends from claim 15, and as a dependent claim therefrom, claim 16 is allowable for the reasons claim 15 is allowable. Appellants further submit that claim 16 is also allowable in light of the presence of novel and non-obvious elements contained in claim 16 that are not otherwise present in claim 15.

m. Claim 17

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 17 subject matter including, *inter alia*,

> "... storing operands of an instruction executing on e round of said DES algorithm in said first, second and third registers using said logic circuit and said shift circuit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction."

(claim 17). Appellants submit that for the same or similar reasons discussed above regarding the reasons why Jones does not disclose, teach or suggest Appellants' claim 7 subject matter, that Jones also does not disclose, teach or suggest Appellants' claim 17 subject matter. Therefore, Appellants submit that Jones cannot and does not disclose, teach or suggest Appellants' claimed subject matter.

Appellants submit that at least because claim 17 depends from claim 16, and as a dependent claim therefrom, claim 17 is allowable for the reasons claim 16 is allowable. Appellants further submit that claim 17 is also allowable in light of the presence of novel and non-obvious elements contained in claim 17 that are not otherwise present in claim 16.

n. Claim 18

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 18 subject matter including, *inter alia*, "... providing said results as input to said logic circuit without first being written back to said first, second and third registers." (claim 18).

Appellants submit that for the same or similar reasons discussed above regarding the reasons why Jones does not disclose, teach or suggest Appellants' claim 8 subject matter, that Jones also does not disclose, teach or suggest Appellants' claim 18 subject matter. Therefore, Appellants submit that Jones cannot and does not disclose, teach or suggest Appellants' claimed subject matter.

Appellants submit that at least because claim 18 depends from claim 17, and as a dependent claim therefrom, claim 18 is allowable for the reasons claim 17 is allowable. Appellants further submit that claim 18 is also allowable in light of the presence of novel and non-obvious elements contained in claim 18 that are not otherwise present in claim 17.

o. Claim 19

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 19 subject matter including, *inter alia*, "... selecting a subkey from a key for said DES algorithm in a second logic circuit." (claim 19). Appellants repeat the above relevant remarks presented above with respect to claim 11.

p. Claim 20

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 20 subject matter including, *inter alia*, "... operating said second logic circuit in parallel with said logic circuit." (claim 20). Appellants repeat the above relevant remarks.

Appellants submit that for the same or similar reasons discussed above regarding the reasons why Jones does not disclose, teach or suggest Appellants' claim 10 subject matter, that Jones also does not disclose, teach or suggest Appellants' claim 20 subject matter. Therefore, Appellants submit that Jones cannot and does not disclose, teach or suggest Appellants' claimed subject matter.

q. Claim 21

Appellants submit that Jones does not disclose, teach or suggest Appellants' claim 21 subject matter including, *inter alia*, "... selecting a subkey from a key using a key select circuit in said logic circuit." (claim 21). Appellants repeat the above relevant remarks.

r. Claim 22

For the sake of brevity, Appellants reiterate the above relevant remarks. Independent claim 22 recites, among other things, "wherein said register file includes general purpose registers to store at least two of attributes parameters datapath, control, L_i's, R_i's, and subkeys K_i's." In contrast, Jones teaches that the register file 58 is controlled by control unit 60, which decodes instructions from a processing element instruction memory 62. As such, the register file does not store at least two of attributes parameters datapath, namely control, L_i's, R_i's, and subkeys K_i's.

s. Claim 23

Appellants submit that this claim is allowable on its own merits based on the same reasoning presented above with respect to claim 3.

IX. Conclusion

For the reasons advanced above, Appellants submit that the Examiner erred in rejecting pending claims 1, 3-13, and 15-23 and respectfully request reversal of the decision of the Examiner.

Respectfully submitted,

Date: July 8, 2005

By: _____

Patrick B. Law
Registration No. 41,549

VEDDER, PRICE, KAUFMAN &
KAMMHOLZ, P.C.
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7599
FAX: (312) 609-5005

Claims on Appeal

Claim 1. A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations;

wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and

wherein said register file includes general purpose registers.

Claim 3. The method of claim 1, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey.

Claim 4. The computer system of Claim 3, wherein said datum is 64 bits long and said subkey is 48 bits long.

Claim 5. The computer system of Claim 3, wherein said first and second portions each contain one-half number of bits of said datum.

Claim 6. The computer system of Claim 5, wherein each of said first and second portions is 32 bits long.

Claim 7. The computer system of Claim 3, wherein said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction.

Claim 8. The computer system of Claim 7, wherein a bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers.

Claim 9. The computer system of Claim 8, wherein said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit.

Claim 10. The computer system of Claim 1, further comprising a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operating in parallel with said logic circuit.

Claim 11. The computer system of Claim 1, wherein said logic circuit further comprises a circuit for selecting a subkey from a key.

Claim 12. The computer system of Claim 11, wherein said key is 56 bits long.

Claim 13. A process for performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

providing a logic circuit in an arithmetic logic unit; and

performing expansion permutation, S-box substitution and P-box permutation and associated XOR operations in said logic circuit; and

storing operands in a register file; and providing said operands to said logic circuit;

wherein said register file includes general purpose registers.

Claim 15. The process of Claim 13, further comprising: storing operands in a register file; and providing said operands to said logic circuit.

Claim 16. The process of Claim 15, further comprising:

storing a first portion of a datum for said encryption or decryption in first register in said register file;

storing a second portion of said datum for said encryption or decryption in second register in said register file; and

storing a subkey for said encryption or decryption in third register in said register file.

Claim 17. The process of Claim 16, further comprising storing operands of an instruction executing one round of said DES algorithm in said first, second and third registers using said logic circuit and said shift circuit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction.

Claim 18. The process of Claim 17, further comprising providing said results as input to said logic circuit without first being written back to said first, second and third registers.

Claim 19. The process of Claim 13, further comprising selecting a subkey from a key for said DES algorithm in a second logic circuit.

Claim 20. The process of Claim 19, further comprising operating said second logic circuit in parallel with said logic circuit.

Claim 21. The process of Claim 13, further comprising selecting a subkey from a key using a key select circuit in said logic circuit.

Claim 22. A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations;

wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and

wherein said register file includes general purpose registers to store at least two of attributes parameters datapath, control, L_i's, R_i's, and subkeys K_i's.

Claim 23 . The computer system of claim 22, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey.

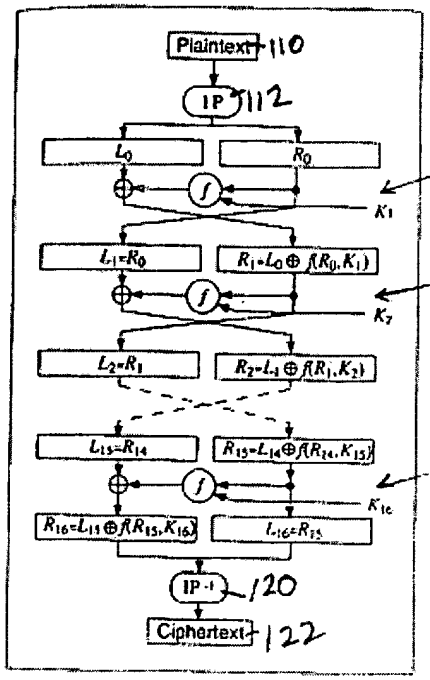


FIG. 1 (PRIOR ART)

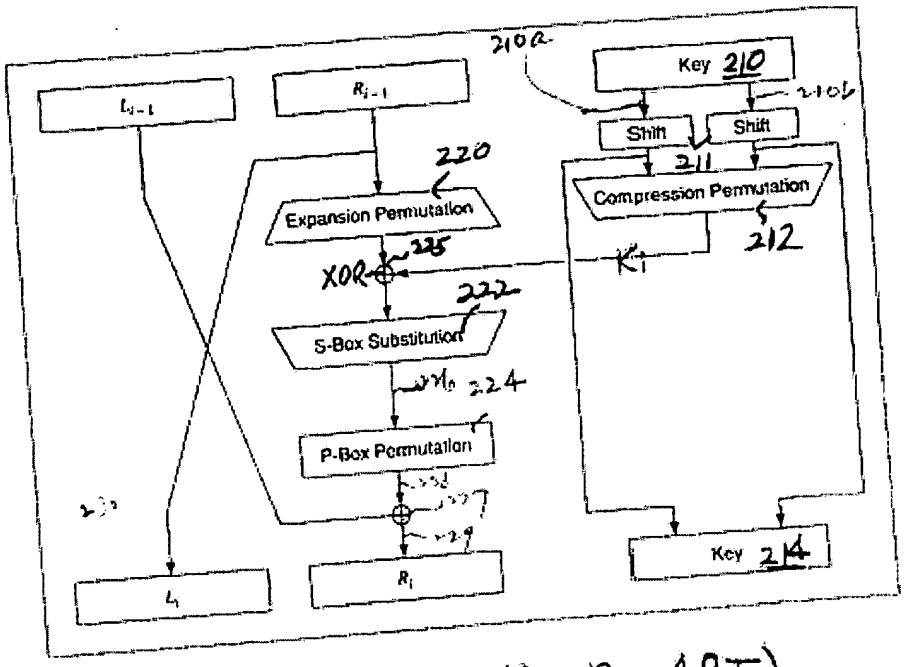


FIG. 2 (PRIOR ART)

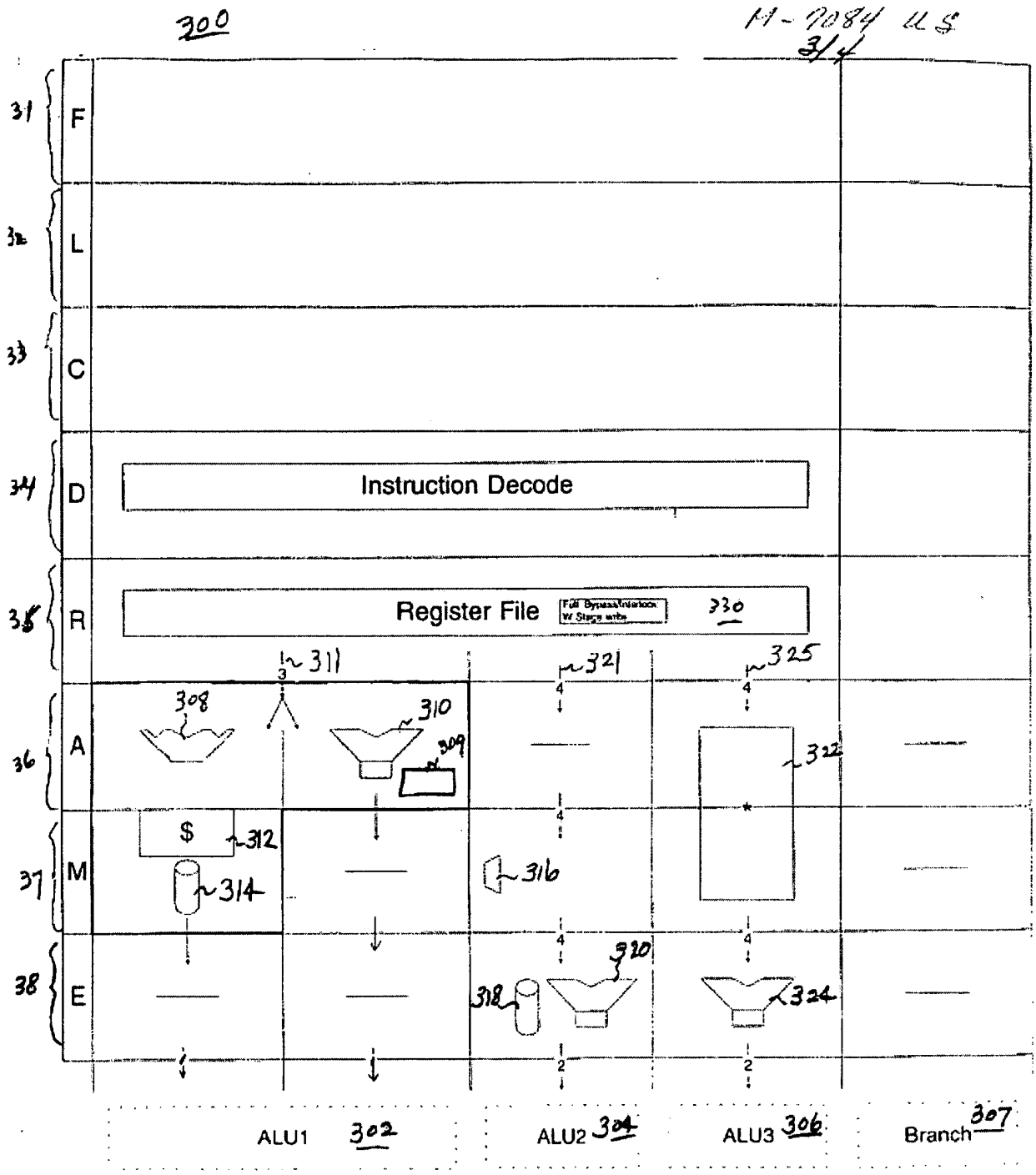

300
M-7084 US
3/4
31
F
32
L
33
C
34
D
Instruction Decode
35
R
Register File
Full Bypass/Interlock W Stage write
330
311
321
325
36
A
308
310
309
322
37
M
$
312
314
316
38
E
318
320
324
ALU1 302
ALU2 304
ALU3 306
Branch 307

FIG. 3

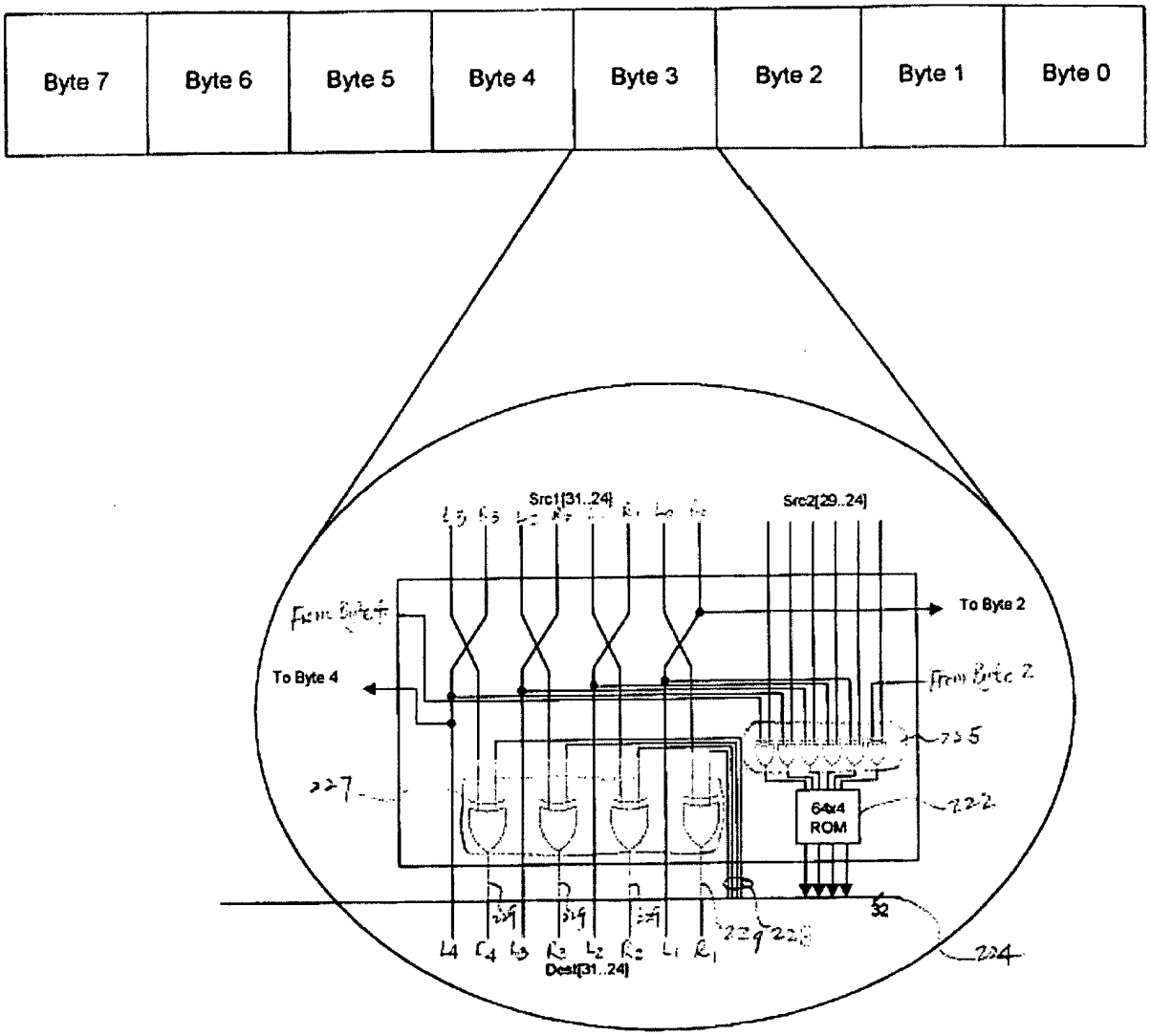


FIG. 4

Appendix B